doi.org/10.51891/rease.v12i9.30426

CONTRAINTELIGÊNCIA CIBERNÉTICA NA PREVENÇÃO DE FRAUDES DIGITAIS: ANTECIPAÇÃO DE COMPORTAMENTOS E PROTEÇÃO DO CONHECIMENTO DEFENSIVO

CYBER COUNTERINTELLIGENCE IN DIGITAL FRAUD PREVENTION: ANTICIPATING BEHAVIOR AND PROTECTING DEFENSIVE KNOWLEDGE

Ialle Teixeira da Conceição[1]

RESUMO: A prevenção de fraudes digitais envolve decisões sobre eventos observáveis e sobre as informações que os próprios mecanismos de proteção disponibilizam a possíveis adversários. Este artigo tem como objetivo propor um modelo conceitual de contrainteligência cibernética que articule a antecipação de comportamentos à proteção do conhecimento defensivo. Desenvolve-se uma pesquisa bibliográfica e documental, de abordagem qualitativa e finalidade propositiva, mediante análise dirigida de oito publicações de inteligência, contrainteligência e análise estruturada. O recorte compreende jornadas digitais de cadastro e autenticação, complementadas por registros públicos de incidentes brasileiros de 2025, sem coleta de dados pessoais ou acesso a informações restritas. A análise identifica relações entre direcionamento da coleta, qualidade das evidências, confronto de hipóteses, proteção de informações sensíveis e revisão das decisões. A partir dessas relações, propõe-se uma matriz que associa conhecimentos a proteger, exposições, indicadores observáveis, explicações concorrentes, avaliação de confiança e respostas defensivas. A aplicação a um cenário hipotético explicita como mudanças de comportamento podem justificar investigação sem constituir, isoladamente, prova de fraude ou de adaptação adversária. Conclui-se que a contribuição da contrainteligência reside na organização de perguntas sobre o aprendizado do adversário e na redução de exposições informacionais evitáveis. O modelo constitui uma proposta analítica ainda não validada empiricamente, cuja avaliação futura deve considerar qualidade das decisões, esforço operacional e efeitos sobre usuários legítimos.

Palavras-chave: Contrainteligência cibernética. Fraudes digitais. Análise estruturada. Conhecimento sensível. Antecipação de ameaças.

[1] Especialista em Engenharia de Software pela Universidade Estácio de Sá e cursando MBA em Cibersegurança pela USP/ESALQ. Universidade de São Paulo (USP/ESALQ).

ABSTRACT: Digital fraud prevention involves decisions about observable events and the information that protective mechanisms themselves make available to potential adversaries. This article proposes a conceptual cyber counterintelligence model that connects behavioral anticipation with the protection of defensive knowledge. It employs qualitative, proposition-oriented bibliographic and documentary research through a focused analysis of eight publications on intelligence, counterintelligence, and structured analysis. Digital registration and authentication journeys are complemented by public records of Brazilian incidents reported in 2025, without personal data collection or access to restricted information. The analysis identifies relationships among collection requirements, evidence quality, competing hypotheses, protection of sensitive information, and decision review. These relationships support a matrix linking knowledge requiring protection, exposure, observable indicators, alternative explanations, confidence assessment, and defensive responses. Application to a hypothetical scenario shows how behavioral changes can warrant investigation without independently proving fraud or adversarial adaptation. The article concludes that counterintelligence contributes by organizing questions about adversarial learning and reducing avoidable information exposure. The model remains an analytical proposal without empirical validation. Future evaluation should examine decision quality, operational effort, and effects on legitimate users.

Keywords: Cyber counterintelligence. Digital fraud. Structured analysis. Sensitive knowledge. Threat anticipation.

1 INTRODUÇÃO

A análise de uma tentativa de fraude digital pode limitar-se à decisão de permitir, interromper ou submeter uma interação a exame adicional. Entretanto, a mesma interação suscita outra pergunta sobre a defesa: quais informações a resposta da organização revelou a quem iniciou a interação? Examinar essa possibilidade amplia o objeto de investigação, incorporando o conhecimento sobre os controles e as condições em que esse conhecimento pode ser obtido por terceiros. O presente artigo explora essa perspectiva em jornadas digitais de cadastro e autenticação.

A questão é relevante porque decisões defensivas e informações sobre seu funcionamento coexistem no mesmo ambiente de interação. Uma resposta ao usuário, uma informação de suporte ou uma documentação técnica podem cumprir uma finalidade legítima e, simultaneamente, oferecer elementos para inferências sobre o processo. Não se presume que toda observação seja maliciosa nem que qualquer detalhe permita contornar uma proteção. Interessa compreender como a exposição de conhecimento pode integrar uma hipótese de risco e quais evidências seriam necessárias para sustentá-la.

A Doutrina da Atividade de Inteligência situa a contrainteligência na proteção de interesses, do processo decisório e de conhecimentos sensíveis diante de ações adversas. Sua

vertente preventiva abrange a identificação de ameaças e vulnerabilidades e o acompanhamento de medidas de proteção (BRASIL, 2023). A aplicação desses conceitos ao ambiente empresarial exige delimitação: as organizações privadas não recebem, por analogia, as competências de órgãos estatais. O aproveitamento proposto restringe-se ao raciocínio analítico, à proteção informacional e à organização de decisões defensivas no próprio ambiente.

A antecipação também exige cuidado conceitual. O planejamento de inteligência trabalha com informações incompletas e procura apoiar decisões oportunas, mantendo explícitas suas limitações (REINO UNIDO, 2023). Desse modo, antecipar comportamentos significa formular possibilidades relevantes, identificar condições que as tornariam mais ou menos plausíveis e acompanhar sua evolução. A atribuição de intenção criminosa a partir de um sinal isolado comprometeria esse propósito, sobretudo quando falhas técnicas e dificuldades de uso também podem produzir comportamentos incomuns.

Heuer Jr. (1999) demonstra que a interpretação de informações é influenciada por expectativas e modelos mentais. Ao favorecer uma explicação inicial, o analista pode desconsiderar dados contraditórios ou atribuir peso excessivo a evidências igualmente compatíveis com alternativas. Em prevenção a fraudes, esse problema oferece uma razão para distinguir o evento observado, a explicação formulada e a ação escolhida. A adoção de técnicas estruturadas permite registrar essas diferenças e submetê-las a revisão, sem eliminar a necessidade de julgamento profissional.

Diante disso, formula-se a seguinte questão: como princípios de contrainteligência e técnicas de análise estruturada podem apoiar a identificação de sinais de adaptação dos fraudadores aos controles de prevenção? O objetivo é propor um modelo conceitual que relacione proteção do conhecimento defensivo, indicadores de possível aprendizado adversário e avaliação de hipóteses concorrentes. A contribuição pretendida consiste em organizar um procedimento examinável, sem alegar previsão determinística de ataques ou eficácia operacional ainda não demonstrada.

2 PROCEDIMENTOS METODOLÓGICOS

O estudo adota pesquisa bibliográfica e documental, com abordagem qualitativa e finalidade propositiva. O *corpus* foi constituído intencionalmente, considerando a pertinência das publicações aos conceitos de contrainteligência, apoio à decisão, qualidade informacional e análise estruturada. Não foi realizada busca exaustiva em bases bibliográficas, razão pela qual

o trabalho não se apresenta como revisão sistemática nem como levantamento completo do estado da arte sobre fraudes digitais.

Foram selecionadas oito obras: a Doutrina da Atividade de Inteligência, da Agência Brasileira de Inteligência; o manual Inteligência Militar Terrestre, EB20-MF-10.107; a publicação britânica JDP 2-00, quarta edição; os documentos norte-americanos MCWP 2-10 e MCRP 2-10A.2; *Psychology of Intelligence Analysis*, de Richards J. Heuer Jr.; *A Tradecraft Primer*; e *Thinking and Writing*, de Robert S. Sinclair. As edições analisadas compreendem o período de 1999 a 2025.

O critério de inclusão foi a presença de fundamentos diretamente relacionados à pergunta de pesquisa. Foram priorizados trechos sobre proteção do conhecimento, necessidades de inteligência, avaliação das evidências, hipóteses alternativas, comunicação e revisão analítica. Documentos centrados em interrogatório ou em ameaças de um país específico foram excluídos do núcleo para evitar deslocamento temático.

A análise foi organizada em três movimentos. Inicialmente, identificaram-se passagens pertinentes nas obras selecionadas, preservando a distinção entre prescrições doutrinárias e reflexões sobre o processo analítico. Em seguida, essas passagens foram comparadas por categorias: direcionamento, proteção informacional, observação, interpretação, decisão e revisão. Finalmente, as relações identificadas foram transpostas para o recorte de cadastro e autenticação, dando origem à matriz e ao cenário ilustrativo apresentados neste artigo. Registros públicos de incidentes brasileiros de 2025 foram examinados apenas como ilustrações contextuais e não integraram o *corpus* doutrinário empregado na construção do modelo.

A unidade de análise corresponde ao argumento ou orientação documental pertinente a cada categoria, e não à frequência de palavras nos textos. Uma recomendação militar sobre definição de necessidades, por exemplo, foi examinada quanto à sua função de orientar decisões antes de ser adaptada ao contexto organizacional. A transposição foi limitada aos elementos compatíveis com uma atuação defensiva. Não foram incorporados procedimentos de operações clandestinas, técnicas de interrogatório ou intervenções em sistemas de terceiros.

Os resultados consistem em síntese interpretativa e proposta de modelo, sem entrevistas, acesso a registros restritos ou observação de campanhas reais. O cenário foi construído para demonstrar o raciocínio e suas limitações; não representa uma amostra, uma simulação estatística ou um experimento. As proposições sobre adaptação de fraudadores são,

portanto, hipóteses analíticas. A seleção intencional e a concentração em fontes doutrinárias limitam a generalização e não permitem estimar a frequência dos comportamentos discutidos.

3 FUNDAMENTOS DA CONTRAINTELIGÊNCIA E DA ANTECIPAÇÃO

3.1 Proteção do conhecimento e limites da transposição

A doutrina brasileira distingue medidas preventivas de contrainteligência e medidas de contraposição a ameaças, ressaltando a interdependência dessas dimensões. A proteção do conhecimento compreende os dados sensíveis, seus detentores, os suportes e os meios de transmissão. Sua abordagem considera governança, pessoas, documentos, tecnologia e instalações, reconhecendo que essas áreas se articulam na prática (BRASIL, 2023, p. 64–66). Essa formulação permite examinar a exposição informacional para além de um componente técnico isolado.

No presente estudo, conhecimento defensivo designa o conjunto de informações que permite compreender como uma organização identifica, avalia e trata interações suspeitas. O termo é empregado como definição operacional do artigo, sem pressupor sua equivalência a uma categoria formal das doutrinas consultadas. Pode abranger critérios internos de decisão, procedimentos de revisão, limitações conhecidas de coleta e detalhes operacionais cuja divulgação desnecessária auxilie inferências sobre a proteção. A sensibilidade deve ser avaliada conforme o contexto e o efeito possível da exposição.

O manual MCRP 2-10A.2 relaciona a contrainteligência à identificação de ameaças, vulnerabilidades, capacidades e intenções adversárias, em um ambiente de atribuições e autoridades específicas (ESTADOS UNIDOS, 2025). Esse enquadramento impede uma adaptação indiscriminada. Em serviços digitais, o objeto pertinente é a possível coleta de conhecimento sobre a defesa e as vulnerabilidades informacionais que a favorecem. Uma anomalia técnica, por si só, não transforma uma investigação antifraude em atividade de contrainteligência.

A distinção tem efeito sobre a seleção das perguntas. Investigar se uma sessão apresenta irregularidades atende a uma necessidade de detecção. Investigar se a sequência de interações pode revelar uma tentativa de compreender o mecanismo defensivo acrescenta uma dimensão de contrainteligência. As duas perguntas podem compartilhar evidências, mas exigem conclusões separadas. É possível suspeitar de fraude sem conhecer qualquer processo de

aprendizado, assim como identificar exposição informacional sem demonstrar exploração maliciosa.

A proteção proposta também deve preservar a capacidade de auditoria e de atendimento. Explicações úteis a usuários e acesso interno necessário ao trabalho não devem ser suprimidos de modo indiscriminado. A revisão deve distinguir a informação suficiente para uma finalidade legítima do detalhe operacional dispensável nessa mesma finalidade. Trata-se de limitar exposições justificadamente sensíveis, mantendo os controles verificáveis e eficazes mesmo quando sua existência geral é conhecida.

3.2 Necessidades de inteligência e oportunidade da decisão

O manual Inteligência Militar Terrestre organiza um ciclo no qual orientação, obtenção, produção e difusão se relacionam às necessidades dos responsáveis pela decisão (BRASIL, 2015). A publicação MCWP 2-10 também vincula requisitos prioritários a decisões relevantes e destaca a necessidade de reavaliar sua utilidade conforme a situação evolui (ESTADOS UNIDOS, 2021, p. 2-6). O aproveitamento desses princípios recomenda iniciar a análise pela decisão que precisa ser apoiada, em vez de acumular registros sem finalidade definida.

No recorte deste artigo, uma necessidade poderia ser formulada da seguinte maneira: quais evidências justificariam revisar a quantidade de informação operacional fornecida em uma etapa de autenticação? A pergunta delimita o conhecimento a proteger, a situação observada e a decisão possível. A partir dela, podem ser definidos os registros necessários, as limitações de obtenção e o momento em que uma avaliação perderia utilidade. A coleta passa a ter relação explícita com uma finalidade defensiva.

A oportunidade da informação é igualmente importante. A JDP 2-00 reconhece que uma avaliação deve chegar em tempo de apoiar a ação, acompanhada das ressalvas pertinentes quanto à confiança (REINO UNIDO, 2023). No ambiente organizacional, isso sugere diferenciar medidas reversíveis de baixo impacto de decisões que afetam de modo relevante o acesso de usuários. Uma evidência limitada pode justificar investigação ou revisão de documentação, sem justificar automaticamente uma restrição definitiva.

Essa diferenciação reduz a dependência de uma certeza impossível. O analista pode reconhecer que uma hipótese permanece inconclusiva e, ainda assim, recomendar a correção de uma exposição desnecessária, desde que a medida seja sustentada pelo diagnóstico da exposição.

A decisão sobre proteger um detalhe interno e a decisão sobre classificar uma pessoa ou sessão como fraudulenta têm objetos e exigências de evidência distintos.

3.3 Vieses e qualidade das evidências

A análise de hipóteses concorrentes apresentada por Heuer Jr. (1999, p. 100–103) orienta o exame de cada evidência em relação às diferentes explicações possíveis. Seu valor está em tornar visíveis as inconsistências e em examinar a capacidade de uma evidência distinguir hipóteses. Uma observação compatível com todas as explicações pode ser importante para descrever a situação, mas contribuir pouco para selecionar uma delas. A transposição desse princípio evita que volume de registros seja confundido com força da conclusão.

O *A Tradecraft Primer* inclui a verificação de pressupostos e da qualidade informacional entre as técnicas de apoio à análise. A avaliação deve considerar a origem, a consistência, a completude e as limitações das informações, além de confrontar hipóteses que poderiam explicar os mesmos dados (ESTADOS UNIDOS, 2009, p. 7–15). No contexto digital, isso implica examinar se o registro representa a interação pretendida, se diferentes fontes estão descrevendo o mesmo evento e se houve alteração no processo de coleta.

A ausência de uma informação também requer interpretação. Heuer Jr. (1999, p. 99) discute a necessidade de perguntar por que uma evidência esperada não está disponível. Aplicado ao problema proposto, um sinal ausente pode decorrer da inexistência do comportamento, de uma limitação de observação ou de uma falha no registro. Antes de utilizar essa ausência para enfraquecer ou fortalecer uma hipótese, é necessário verificar se o sinal seria observável nas condições analisadas.

Sinclair (2010) associa o trabalho analítico à organização do pensamento e à consideração do destinatário durante a escrita. Essa contribuição sustenta o uso de registros que apresentem a conclusão junto de seu fundamento e de suas restrições. Uma avaliação que omite pressupostos pode parecer mais segura do que a evidência permite. A comunicação deve distinguir o que foi observado, o que foi inferido e qual informação poderia alterar o entendimento atual.

4 APRENDIZADO ADVERSÁRIO COMO HIPÓTESE DE INVESTIGAÇÃO

A expressão aprendizado adversário é utilizada neste artigo para representar a hipótese de que um agente ajusta suas ações a partir de informações obtidas em interações anteriores com a organização. Essa definição não pressupõe que o agente disponha de conhecimento completo,

planejamento sofisticado ou capacidade de observar todos os controles. O comportamento pode ser fragmentado, condicionado por recursos disponíveis e influenciado por interpretações incorretas. A investigação precisa preservar essas possibilidades para não atribuir racionalidade excessiva ao adversário.

Para fins analíticos, podem ser consideradas interações de observação, experimentação e adaptação. Na observação, o agente potencialmente obtém informações sobre o processo. Na experimentação, as interações apresentam variações que poderiam servir à comparação de respostas. Na adaptação, o comportamento se modifica de forma compatível com algum aprendizado anterior. Essas categorias descrevem relações possíveis; não constituem etapas universais nem uma sequência empiricamente demonstrada por este estudo.

A ordem temporal é relevante, mas não estabelece causalidade. Uma mudança posterior à atualização de um controle pode sugerir uma hipótese de adaptação, porém também pode decorrer de alterações de interface, instabilidade, sazonalidade ou composição diferente dos acessos. Para sustentar a relação, seria necessário investigar se o grupo observado foi exposto à mudança, se a coleta permaneceu comparável e se explicações alternativas foram examinadas. A coincidência temporal deve iniciar uma pergunta, e não encerrá-la.

A unidade observada exige cuidado semelhante. Sessões diferentes não representam necessariamente pessoas diferentes, e uma característica compartilhada não prova atuação coordenada. Ao agregar eventos, a investigação deve justificar os critérios de associação e registrar suas limitações. Caso contrário, a própria forma de agrupamento pode produzir uma aparência de campanha. A independência das evidências precisa ser examinada antes de se atribuir maior confiança à repetição de um padrão.

A proteção informacional pode considerar, como exemplos analíticos, respostas externas excessivamente detalhadas, documentos com critérios internos disponíveis além do necessário e circulação descontrolada de orientações operacionais. O risco depende de conteúdo, acessibilidade e possibilidade de utilização. A existência de documentação pública, por exemplo, não é uma falha em si. A pergunta relevante é se o material permite inferir conhecimento sensível que não é necessário ao seu propósito legítimo.

O monitoramento de indicadores, conforme discutido no *A Tradecraft Primer*, torna explícitas as condições que poderiam acompanhar o desenvolvimento de um cenário e permite revisar sua plausibilidade ao longo do tempo (ESTADOS UNIDOS, 2009, p. 12–15). A aplicação proposta inclui indicadores favoráveis e contrários à hipótese de aprendizado. A constatação de

um defeito de interface capaz de explicar a interrupção de sessões, por exemplo, deve reduzir a centralidade da explicação adversária quando a evidência for pertinente.

A antecipação resulta, assim, da capacidade de preparar perguntas e respostas condicionais. Em vez de afirmar que o fraudador executará uma ação específica, a avaliação registra quais mudanças justificariam atenção, quais evidências seriam esperadas e em que circunstâncias a hipótese deveria ser abandonada. Esse procedimento cria condições para uma resposta oportuna, mas sua utilidade depende da qualidade da observação e da disposição institucional para revisar conclusões.

5 MODELO CONCEITUAL DE CONTRAINTELIGÊNCIA CIBERNÉTICA

A síntese documental articula a proteção do conhecimento discutida na doutrina brasileira, o direcionamento por necessidades presente nos manuais militares e as técnicas de avaliação de hipóteses desenvolvidas na literatura analítica (BRASIL, 2015; BRASIL, 2023; ESTADOS UNIDOS, 2009; HEUER JR., 1999). Dessa articulação deriva a matriz apresentada no Quadro 1. A organização em seis componentes é uma proposta deste artigo e não corresponde a um modelo integral reproduzido de uma das fontes.

Quadro 1 – Componentes da matriz proposta

Componente	Pergunta orientadora	Registro esperado
Conhecimento defensivo	O que precisa ser protegido e por quê?	Informação sensível e efeito possível da exposição.
Exposição	Por qual meio o conhecimento pode ficar acessível?	Canal, alcance e finalidade legítima.
Indicador observável	Qual evento justificaria investigar a hipótese?	Observação delimitada no tempo e sua fonte.
Hipóteses concorrentes	Quais explicações permanecem plausíveis?	Alternativas adversárias, técnicas e de uso legítimo.
Avaliação analítica	O que sustenta ou enfraquece cada explicação?	Evidências, lacunas e justificativa da confiança.
Resposta e revisão	Qual ação cabe e quando reavaliá-la?	Responsável, medida e condição de revisão.

Fonte: elaboração própria, a partir de Brasil (2015; 2023), Estados Unidos (2009; 2021) e Heuer Jr. (1999).

5.1 Delimitação do conhecimento e da exposição

O primeiro componente requer especificar a informação a proteger e o motivo de sua sensibilidade. Expressões abrangentes, como proteger o sistema inteiro, dificultam a análise porque não estabelecem o que poderia ser conhecido nem o efeito da exposição. Uma delimitação mais útil identifica uma informação operacional concreta e a decisão que ela pode influenciar, preservando o nível de detalhe apropriado ao documento de análise.

O segundo componente identifica onde essa informação circula e quem necessita acessá-la. A revisão deve considerar finalidade, destinatários e manutenção do conteúdo, pois uma informação adequada a uma atividade pode ser excessiva em outra. Também é necessário registrar o custo da restrição: impedir o acesso de uma equipe que precisa investigar incidentes pode enfraquecer a defesa. A classificação precisa orientar o uso responsável, em vez de produzir sigilo indiscriminado.

A combinação desses componentes permite distinguir vulnerabilidade informacional de exploração confirmada. Se uma resposta externa revela detalhe desnecessário, a exposição pode ser documentada e tratada mesmo sem identificar fraude. A afirmação de que um agente utilizou aquele detalhe exige evidência adicional. Essa separação impede que uma medida razoável de prevenção seja apresentada como comprovação retrospectiva de intenção adversária.

5.2 Indicadores e confronto de hipóteses

O indicador deve ser descrito em termos observáveis, com delimitação temporal e condições de obtenção. Registrar sessões encerradas em determinada etapa é diferente de registrar reconhecimento malicioso: a primeira formulação descreve um evento; a segunda já incorpora uma interpretação. A matriz preserva a observação antes de associá-la a uma hipótese, permitindo que explicações sejam revistas sem alterar o fato documentado.

As hipóteses devem abranger alternativas plausíveis e distinguir explicações que podem coexistir. Um defeito técnico pode afetar usuários legítimos enquanto um agente malicioso explora o mesmo ambiente. Quando as alternativas não forem mutuamente exclusivas, essa condição precisa ser registrada. O objetivo não é forçar toda ocorrência a uma classificação única, mas identificar quais explicações encontram apoio e quais informações adicionais têm valor para a decisão.

O confronto considera evidências favoráveis, contraditórias e sem capacidade discriminante. Também examina se diferentes registros derivam da mesma fonte e se pressupostos estão sendo tratados como fatos. A simples soma de sinais pode superestimar uma hipótese quando todos refletem um único evento. Recomenda-se registrar o vínculo entre os dados e testar se a conclusão permanece defensável quando uma evidência decisiva é retirada ou considerada incorreta.

A confiança atribuída deve refletir qualidade e suficiência das informações, sem ser convertida automaticamente em uma probabilidade numérica. Uma descrição de baixa confiança pode indicar lacunas de observação; uma avaliação mais sustentada deve explicar quais fontes e verificações permitem essa qualificação. O nome da categoria, isoladamente, pouco informa. O elemento indispensável é a justificativa, acompanhada das condições que poderiam modificar a conclusão.

5.3 Resposta proporcional e revisão

A escolha da resposta deve considerar o objeto da decisão e as consequências de um erro. Revisar documentação excessivamente detalhada, corrigir uma falha de coleta e impedir o acesso de um usuário têm impactos distintos. A matriz deve identificar o responsável, o fundamento da medida e o momento de revisão. A associação entre análise e ação segue o princípio de utilidade decisória presente nos documentos militares, adaptado às responsabilidades organizacionais (ESTADOS UNIDOS, 2021; REINO UNIDO, 2023).

Recomenda-se manter separadas a avaliação de intenção e a avaliação de exposição. A primeira pode continuar inconclusiva enquanto a segunda sustenta uma melhoria de proteção. Também é possível que a investigação identifique apenas um problema de usabilidade, caso em que a contribuição relevante será corrigir o processo e reduzir suspeitas indevidas. Um modelo de antecipação precisa reconhecer esses resultados, sem considerar o descarte de uma hipótese adversária como fracasso analítico.

A revisão deve ocorrer diante de novas evidências, alteração relevante do ambiente ou vencimento do prazo definido para a avaliação. O registro anterior precisa ser preservado para permitir comparação entre o que se sabia e o que foi conhecido depois. Essa prática favorece a aprendizagem institucional e evita que uma explicação posterior seja tratada como se estivesse disponível desde o início. A continuidade do processo depende dessa memória, e não apenas da existência de alertas.

6 APLICAÇÃO ILUSTRATIVA E DISCUSSÃO

6.1 Incidentes brasileiros recentes como contexto

Os incidentes divulgados no Brasil em 2025 ajudam a delimitar problemas distintos que podem convergir na proteção de serviços financeiros digitais. O Banco Central comunicou a exposição de um conjunto limitado de dados cadastrais associados a chaves Pix sob responsabilidade da QI Sociedade de Crédito Direto. Segundo o comunicado, o acesso não autorizado ocorreu entre 23 de fevereiro e 6 de março de 2025. A autoridade esclareceu que não foram acessados senhas, saldos ou dados de movimentação e que as informações expostas não permitiam, por si sós, realizar pagamentos; ainda assim, advertiu para seu possível emprego em tentativas posteriores de golpe ou obtenção de dados adicionais (BANCO CENTRAL DO BRASIL, 2025). O caso demonstra por que exposição informacional e movimentação financeira indevida devem ser avaliadas separadamente.

Em julho de 2025, o ataque relacionado à C&M Software atingiu a infraestrutura de mensageria utilizada por instituições financeiras e de pagamento. Balanço da Polícia Federal divulgado pela imprensa atribuiu ao esquema desvios superiores a R$ 813 milhões e registrou a venda de credenciais de acesso por um operador de tecnologia; a C&M declarou ter sido vítima de ação criminosa com uso de credenciais (CNN BRASIL, 2025). Para o modelo proposto, o episódio desloca a atenção do comportamento do cliente final para a cadeia de terceiros, o acesso privilegiado, a criação ou uso de credenciais e a capacidade de identificar movimentações incompatíveis com o contexto operacional.

No mês seguinte, outro incidente público envolveu a Sinqia, provedora de tecnologia do sistema financeiro. Reportagem da Reuters informou que o evento alcançou o ambiente Pix e foi associado a transferências não autorizadas envolvendo instituições atendidas pela empresa (REUTERS, 2025). As informações disponíveis publicamente não autorizam concluir que os episódios da C&M e da Sinqia tiveram a mesma causa, os mesmos agentes ou controles equivalentes. Sua consideração conjunta é útil apenas para evidenciar a concentração de risco em prestadores com conectividade sensível e a necessidade de hipóteses que abranjam credenciais, dependências tecnológicas e resposta coordenada.

Esses casos ampliam o recorte originalmente centrado em cadastro e autenticação. Em *fintechs* e instituições conectadas ao Sistema de Pagamentos Brasileiro, o conhecimento defensivo também inclui topologia de integrações, privilégios de contas técnicas, procedimentos

de aprovação, limites operacionais e rotinas de resposta. O monitoramento deve procurar sinais favoráveis e contrários a hipóteses de comprometimento, sem confundir vazamento cadastral, fraude induzida contra clientes, abuso interno e invasão de infraestrutura. A classificação correta do fenômeno condiciona tanto a coleta quanto a resposta proporcional.

6.2 Cenário hipotético de cadastro e autenticação

Considere-se, exclusivamente para ilustração, uma organização que identifica aumento de sessões interrompidas em uma etapa de autenticação após uma mudança em seu processo. Algumas interações também apresentam variações de características do ambiente. Na mesma ocasião, a revisão interna identifica que uma resposta externa contém detalhes operacionais dispensáveis ao atendimento. Nenhum desses elementos representa observação realizada nesta pesquisa; o cenário foi construído para exercitar o modelo.

A primeira hipótese considera tentativa de compreender o controle e adaptar o comportamento. A segunda considera dificuldade legítima de uso. A terceira examina uma falha técnica ou de registro. Essas explicações não são necessariamente exclusivas. A análise inicial deve, portanto, delimitar quais sessões pertencem a cada comparação, quais dados estão disponíveis e se a mudança de processo alterou a própria produção dos registros.

O Quadro 2 exemplifica como o mesmo conjunto de observações pode exigir verificações distintas. A finalidade não é atribuir pontuações nem selecionar antecipadamente uma hipótese vencedora. O exercício demonstra que a capacidade de discriminação depende de informações adicionais e que uma exposição identificada pode justificar tratamento independentemente da conclusão sobre intenção.

Quadro 2 – Exame de observações em cenário hipotético

Observação ilustrativa	Limite da interpretação	Verificação necessária
Interrupções após mudança	Sucessão temporal não demonstra adaptação.	Comparabilidade da coleta e efeitos da mudança.
Variações entre sessões	Variação não prova coordenação ou fraude.	Critérios de associação e explicações legítimas.
Detalhe operacional exposto	Exposição não comprova utilização adversária.	Conteúdo, acessibilidade e necessidade de divulgação.

Observação ilustrativa	Limite da interpretação	Verificação necessária
Ausência de sinal esperado	Ausência pode refletir falha de observação.	Condições técnicas para produzir o registro.

Fonte: elaboração própria. Todas as observações são hipotéticas.

Uma resposta inicial justificável seria corrigir a exposição desnecessária, examinar a alteração técnica e manter a hipótese adversária em acompanhamento. Essa resposta não exige afirmar que todas as sessões são fraudulentas. Se uma falha de interface explicar parte das interrupções, a análise deve incorporar o achado e rever o alcance da suspeita. Se a hipótese de aprendizado permanecer plausível, o registro deve explicitar as lacunas que impedem uma conclusão mais firme.

O exercício também evidencia um limite: a matriz organiza perguntas, mas não produz informações que o ambiente não registra. Uma investigação pode terminar sem distinguir as explicações. Nessa situação, a conclusão apropriada deve informar a insuficiência de evidência e indicar a coleta proporcional necessária para uma avaliação futura. Transformar a incerteza em acusação apenas para concluir o processo contrariaria o fundamento analítico da proposta.

6.3 Contribuições organizacionais e formação dos analistas

A principal contribuição conceitual consiste em reunir dois objetos frequentemente tratados separadamente na investigação: o comportamento observado e o conhecimento defensivo potencialmente exposto. A ligação entre eles permite perguntar se a resposta institucional fornece informações relevantes para novas tentativas. Essa relação é uma interpretação proposta a partir do *corpus*; as fontes doutrinárias não demonstram, por si mesmas, sua eficácia em serviços financeiros digitais.

A aplicação também depende da formação dos profissionais. Heuer Jr. (1999) e Sinclair (2010) oferecem fundamentos para discutir pressupostos, organização do raciocínio e comunicação das avaliações. Exercícios com cenários podem solicitar que analistas distingam fatos de inferências, apresentem alternativas e indiquem evidências capazes de modificar seu entendimento. O desempenho deve considerar a justificativa apresentada e a capacidade de revisão, evitando premiar apenas conclusões firmes ou a identificação de uma ameaça.

A discussão entre áreas é necessária porque uma interpretação suspeita pode ser esclarecida por conhecimento operacional que não está nos registros. Equipes responsáveis pela experiência do usuário, manutenção e atendimento podem explicar alterações legítimas. O compartilhamento deve manter a finalidade da investigação e o acesso pertinente, sem expor desnecessariamente detalhes sensíveis. A própria coordenação passa a integrar a proteção do conhecimento, pois informações dispersas ou contraditórias dificultam decisões fundamentadas.

A matriz ainda pode contribuir para a memória institucional ao preservar versões das avaliações. Quando uma hipótese é descartada, o motivo do descarte pode orientar investigações futuras e reduzir repetição de erros. Quando permanece inconclusiva, a lacuna documentada permite decidir se vale investir em observação adicional. Em ambos os casos, o registro oferece um produto útil, embora não corresponda à confirmação de fraude.

6.4 Limitações e agenda de validação

A pesquisa não permite afirmar que o modelo reduz perdas, diminui falsos positivos ou antecipa ações de fraudadores. O *corpus* foi selecionado por pertinência e reúne tradições institucionais distintas, predominantemente voltadas à inteligência estatal e militar. Essa origem limita a transposição para relações de consumo e serviços digitais. Além disso, não foram incorporados resultados de uma revisão abrangente da literatura empírica sobre fraude, o que restringe afirmações sobre frequência e causalidade dos comportamentos.

As técnicas estruturadas também dependem de escolhas humanas. Uma hipótese relevante pode ser omitida, uma fonte pode receber confiança indevida e a matriz pode apenas formalizar uma interpretação inicial. Sua utilização não elimina vieses. Por essa razão, o procedimento deve admitir contestação, revisão dos pressupostos e abandono de categorias que não auxiliem a decisão. O preenchimento completo de um formulário não equivale à qualidade analítica.

Uma avaliação futura poderia comparar investigações realizadas com e sem o protocolo, utilizando casos com desfechos conhecidos e preservando as informações disponíveis no momento original da decisão. A distribuição dos casos deveria considerar diferenças de dificuldade e experiência dos participantes, evitando que a familiaridade com o desfecho favorecesse artificialmente uma abordagem. O desenho e os critérios de avaliação precisariam ser definidos antes da comparação.

Entre as medidas possíveis estão concordância com desfechos confiáveis, tempo de análise, proporção de conclusões com evidências rastreáveis e frequência de revisões justificadas. Resultados inconclusivos devem permanecer identificados, pois sua exclusão pode produzir uma impressão indevida de acerto. Uma eventual redução no número de alertas também precisa ser examinada junto da capacidade de reconhecer ocorrências relevantes, para que menor volume não seja confundido com melhor proteção.

Por fim, a avaliação deve considerar efeitos sobre usuários legítimos e custos da restrição de informação. Proteger conhecimento defensivo pode exigir revisão de comunicação, mas o excesso de opacidade pode prejudicar atendimento e correção de erros. O modelo precisa ser examinado segundo sua utilidade para decisões justificáveis, e não apenas pela capacidade de ampliar monitoramento. Seu valor dependerá do equilíbrio entre informação suficiente, proteção pertinente e possibilidade de revisão.

7 CONSIDERAÇÕES FINAIS

O artigo propôs um modelo conceitual de contrainteligência cibernética para relacionar antecipação de comportamentos e proteção do conhecimento defensivo em jornadas digitais de cadastro e autenticação e em dependências tecnológicas de serviços financeiros. A análise documental permitiu organizar essa relação em componentes que abrangem o conhecimento sensível, sua exposição, os indicadores observáveis, as hipóteses concorrentes, a avaliação e a resposta. A contribuição está na explicitação do raciocínio que liga uma observação à decisão de investigar ou proteger determinada informação.

A pergunta de pesquisa foi respondida no plano conceitual: princípios de contrainteligência orientam a identificação do que pode ser conhecido pelo adversário, enquanto técnicas estruturadas ajudam a avaliar se os eventos observados sustentam uma hipótese de aprendizado. Antecipação, nessa perspectiva, consiste em acompanhar condições e revisar cenários. A presença de um padrão incomum não basta para concluir intenção fraudulenta, e a exposição de uma informação não comprova sua exploração.

A aplicação ilustrativa mostrou a importância de separar o tratamento de uma vulnerabilidade informacional da classificação de uma interação como maliciosa. A organização pode corrigir uma exposição documentada enquanto mantém inconclusiva a hipótese sobre o agente. Também pode identificar uma falha técnica e abandonar a explicação adversária. Essas possibilidades preservam a coerência entre a evidência disponível e o alcance da ação escolhida.

O modelo permanece sem validação empírica. Sua continuidade exige investigação aplicada que examine qualidade das decisões, esforço de análise e consequências para usuários legítimos. A proteção do conhecimento defensivo será útil na medida em que apoie decisões verificáveis e preserve a disposição para corrigir avaliações. Esse compromisso com a revisão oferece uma base para aproximar fundamentos de contrainteligência das necessidades concretas de prevenção a fraudes digitais.

REFERÊNCIAS

BANCO CENTRAL DO BRASIL. Banco Central comunica ocorrência em instituição. Brasília, DF, 2025. Disponível em: <https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Incidentes%20DICT/BC_comunica_ocorrencia_Pix-18.pdf>. Acesso em: 9 set. 2026.

BRASIL. Agência Brasileira de Inteligência. *Doutrina da atividade de inteligência*. Brasília, DF: ABIN, 2023. Disponível em: <https://www.gov.br/abin/pt-br/assuntos/escola-de-inteligencia/arquivos_pdf/doutrina-da-atividade-de-inteligencia-2023.pdf>. Acesso em: 9 set. 2026.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. *Inteligência militar terrestre*: EB20-MF-10.107. 2. ed. Brasília, DF: Estado-Maior do Exército, 2015. Disponível em: <https://cdoutex.eb.mil.br/images/painel/pdf/EB20MF10107.pdf>. Acesso em: 9 set. 2026.

CNN BRASIL. PF prende 21 pessoas responsáveis por ataque hacker que afetou Pix. Brasília, DF, 31 out. 2025. Disponível em: <https://www.cnnbrasil.com.br/nacional/brasil/pf-prende-21-pessoas-responsaveis-por-ataque-hacker-que-afetou-pix/>. Acesso em: 9 set. 2026.

ESTADOS UNIDOS. Governo dos Estados Unidos. *A tradecraft primer*: structured analytic techniques for improving intelligence analysis. [S.l.]: Governo dos Estados Unidos, 2009. Disponível em: <https://www.cia.gov/resources/csi/static/Tradecraft-Primer-apr09.pdf>. Acesso em: 9 set. 2026.

ESTADOS UNIDOS. Marine Corps. *Intelligence operations*: MCWP 2-10. [S.l.]: U.S. Marine Corps, 2021. Disponível em: <https://www.marines.mil/Portals/1/Publications/MCWP%202-10.pdf>. Acesso em: 9 set. 2026.

ESTADOS UNIDOS. Marine Corps. *Counterintelligence and human intelligence*: MCRP 2-10A.2. [S.l.]: U.S. Marine Corps, 2025. Disponível em: <https://www.marines.mil/Portals/1/Publications/MCRP%202-10A.2%20%28SECURED%29.pdf>. Acesso em: 9 set. 2026.

HEUER JR., Richards J. *Psychology of intelligence analysis*. [S.l.]: Center for the Study of Intelligence, Central Intelligence Agency, 1999. Disponível em: <https://www.cia.gov/resources/csi/static/Pyschology-of-Intelligence-Analysis.pdf>. Acesso em: 9 set. 2026.

REINO UNIDO. Ministry of Defence. *Intelligence, counter-intelligence and security support to joint operations*: Joint Doctrine Publication 2-00. 4. ed. [S.l.]: Development, Concepts and Doctrine Centre, 2023. Disponível em: <https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf>. Acesso em: 9 set. 2026.

REUTERS. Hackers roubam pelo menos R$ 400 mi do HSBC em ataque que envolve Sinqia, diz NeoFeed. UOL Tilt, 30 ago. 2025. Disponível em: <https://www.uol.com.br/tilt/noticias/reuters/2025/08/30/hackers-roubam-pelo-menos-r400-mi-do-hsbc-em-ataque-que-envolve-sinqia-diz-neofeed.htm>. Acesso em: 9 set. 2026.

SINCLAIR, Robert S. *Thinking and writing*: cognitive science and intelligence analysis. Edição revista. Washington, DC: Center for the Study of Intelligence, 2010. Disponível em: <https://www.cia.gov/resources/csi/static/9e870ec099fc6192e2e412bee248257e/Thinking-and-Writing.pdf>. Acesso em: 9 set. 2026.